NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

North Dakota

Former soldier pleads guilty in militia case. A former Army medic pleaded guilty October 15 to charges that he burned bloody clothes, spent shotgun shells, and a cellphone to try to help fellow soldiers cover up a double killing that prosecutors say was linked to a militia group plotting terrorist attacks while operating inside the military at Fort Stewart in southeast Georgia. The former private first-class of Fargo, North Dakota, told a Liberty County Superior Court judge that he built the backyard bonfire used to dispose of the items December 2011. Source: http://www.militarytimes.com/news/2012/10/ap-former-soldier-pleads-guilty-militia-plot-stewart-101512/

Regional

Nothing Significant to Report

National

(New York) **U.S. President was considered potential target.** A Bangladeshi man snared in an FBI terror sting considered targeting the U.S. President and the New York City Stock Exchange before plotting a car bomb attack on the Federal Reserve, a law enforcement official told the Associated Press October 18. The official stressed that the suspect never got beyond the discussion stage in considering an attack on the U.S. President. In a September meeting with an undercover agent posing as a fellow jihadist, the suspect explained he chose the Federal Reserve as his car bomb target "for operational reasons," according to a criminal complaint. The suspect also indicated he knew that choice would "cause a large number of civilian casualties, including women and children," the complaint said. FBI agents grabbed the man — armed with a cellphone he believed was rigged as a detonator — after he made several attempts to blow up a fake 1,000-pound the bomb inside a vehicle parked next to the Federal Reserve October 17 in lower Manhattan, the complaint said. The suspect appeared in federal court October 17 to face charges of attempting to use a weapon of mass destruction and attempting to provide material support to a terrorist group. Source: http://abcnews.go.com/US/wireStory/feds-indicted-plot-attack-federal-reserve-17502296#.UIAqjK74LxM

International

US Embassy Evacuated in Stockholm. The U.S. Embassy in Stockholm, Sweden, was evacuated October 16 after receiving a letter containing an unknown substance, police said. Bomb disposal experts were sent to the embassy to remove the letter and analyze its contents. Streets around the embassy were closed, but reopened after police removed the letter. Police declined to give details on the content but a police spokesman told Swedish tabloid Expressen it contained some kind of "powder." It may have been dangerous, but it's not dangerous now," he added. An embassy spokesman said the embassy was evacuated and officials were investigating "a possible security incident" together with Swedish authorities, but declined to give other details. Source: http://abcnews.go.com/International/wireStory/us-embassy-evacuated-stockholm-17497869#.UH60aKCBxI1

14 Mexican cops now detained for attack on U.S. Embassy vehicle. Two more police officers were arrested in connection with the attack in August on a U.S. Embassy vehicle, bringing the number of law enforcement agents detained in the course of the investigation to 14, Mexico's Attorney General said. Twelve officers were initially arrested and placed in preventative detention, with two more now detained because they were present when the incident occurred and can provide statements to investigators, he said in a press conference October 13. August 24, two U.S. Embassy officials and a Mexican marine were shot and wounded by Federal Police officers while traveling in an armored SUV with diplomatic plates on a road in the central State of Morelos. The officers involved in the shooting were investigating the kidnapping of a federal official, the Public Safety Secretariat said earlier in October. The U.S. Embassy in Mexico City initially described the incident as an "ambush." A judge initially ordered the 12 officers held under "arraigo," a controversial instrument under which Mexican authorities can hold people linked to serious crimes for up to 80 days without formal charges, for 40 days while they are investigated for alleged "abuse of authority" and other crimes. The results of the investigation will be released before the 40-day period expires, the Attorney General said. Investigators are looking at the possibility that the detained officers may have had links to organized crime groups, he said. Source: http://latino.foxnews.com/latino/news/2012/10/14/14-mexican-cops-now-detained-for-attack-on-us-embassy-vehicle/

Banking and Finance Industry

CapOne takes second DDoS hit. Capital One confirmed that its Web site was hit by another distributed denial of service (DDoS) attack, October 16. The incident was the second attack allegedly waged in October by a hacktivist group against the bank. "Capital One is experiencing intermittent access to some online systems due to a denial of service attack," a bank spokeswoman said. "There was minimal impact to the majority of our customers." The same day, a post claiming to be from the hacktivist group appeared on Pastebin claiming new attacks against U.S. banks would be waged between October 16 and October 18. The group noted that this new wave of DDoS attacks is being initiated without advance warning. In earlier Pastebin posts, the group named the eight banks it eventually attacked. A financial fraud and security consultant with CEB TowerGroup said the October 9 attack against Capital One, appeared to be one of the most damaging. "With CapOne, they seemed to take a bigger hit than the others," he said. "Other banks seemed to handle the attacks better." Source: http://www.bankinfosecurity.com/capone-takes-second-ddos-hit-a-5203

U.S. nuclear outages seen down a third next spring. About 18,800 megawatts (MW) of power capacity at U.S. nuclear operators are expected to be offline at the peak of the 2013 spring refueling season, down roughly a third from the 2012 season, Reuters reported October 16. The data assumes units currently on extended outages, such as the two at Southern California Edison's 2,150-MW San Onofre plant in California, Progress Energy Florida's 860-MW Crystal River in Florida, and Omaha Public Power District's 478-MW Fort Calhoun in Nebraska, will still be shut. Nuclear outages over the past five years have averaged about 23,200 MW in spring and 22,200 MW in the autumn. Since 1999, spring outages have peaked near 32,800 MW in 2011 and bottomed at 16,100 MW in 2004. Autumn outages peaked near 27,200 MW in 2009 and bottomed at about 12,300 MW in 2004. Source: http://www.chicagotribune.com/business/sns-rt-us-utilities-nuclear-outages-springbre89f1cc-20121016,0,6387721.story

New scam pilfers social security checks at banks. A new scam is diverting Social Security checks from seniors by re-routing the checks using direct deposit systems at banks, the Associated Press reported October 14. Scammers typically gain the name and bank account number of victims through phony lottery and sweepstakes schemes. Then the scammers call the Social Security Administration (SSA) posing as the victims and re-route the checks to an account the scam artists can tap. The SSA has found more than 19,000 unauthorized attempts to change direct deposit accounts and receives another 50 each day. Source: http://www.myfoxny.com/story/19814917/new-scam-pilfers-social-security-checks-at-banks

Chemical and Hazardous Materials Sector

Nuclear power plants located in tsunami risk zones. Scientists have highlighted “potentially dangerous” areas that are home to completed nuclear plants or those under construction. The study is the first to look into the location of nuclear power plants and correlate them to areas at risk of tsunamis. “We are dealing with the first vision of the global distribution of civil nuclear power plants situated on the coast and exposed to tsunamis,” explained a co-author of the study and researcher at the Centre for Research on the Epidemiology of Disasters of the Catholic University of Leuven in Belgium. To inform their analysis, the authors used historical, archaeological, geological, and instrumental records as a base for determining tsunami risk. Their study presented a map of the world’s geographic zones that are more at risk of large tsunamis. Based on these data, 23 nuclear power plants with 74 reactors have been identified in high-risk areas. One of them includes Fukushima I. Of these, 13 plants with 29 reactors are active; another 4, that now have 20 reactors, are being expanded to house 9 more; and there are 7 new plants under construction with 16 reactors. Despite the fact that the risk of these natural disasters threatens practically the entire western coast of the American continent. Source: http://phys.org/news/2012-10-nuclear-power-tsunami-zones.html

U.S. nuclear outages seen down a third next spring. About 18,800 megawatts (MW) of power capacity at U.S. nuclear operators are expected to be offline at the peak of the 2013 spring refueling season, down roughly a third from the 2012 season, Reuters reported October 16. The data assumes units currently on extended outages, such as the two at Southern California Edison’s 2,150-MW San Onofre plant in California, Progress Energy Florida’s 860-MW Crystal River in Florida, and Omaha Public Power District’s 478-MW Fort Calhoun in Nebraska, will still be shut. Nuclear outages over the past five years have averaged about 23,200 MW in spring and 22,200 MW in the autumn. Since 1999, spring outages have peaked near 32,800 MW in 2011 and bottomed at 16,100 MW in 2004. Autumn outages peaked near 27,200 MW in 2009 and bottomed at about 12,300 MW in 2004. Source:

http://www.chicagotribune.com/business/sns-rt-us-utilities-nuclear-outages-springbre89f1cc-20121016,0,6387721.story

Commercial Facilities

(Florida) **Police ID gunman in Casselberry salon mass shooting.** Police provided the name of the gunman who stormed into a Casselberry, Florida salon October 18 and shot four women — killing three — before driving away and committing suicide. The suspect killed his ex-girlfriend, the salon manager, and several of her coworkers at the Las Dominicanas M & M Salon on Aloma Avenue. Both the salon manager and the owner of the salon filed domestic violence injunctions against the suspect in recent weeks. He was supposed to report to the Orange County Courthouse October 18 for a hearing in the domestic violence case. A fourth employee was taken to an area hospital, and her condition is unknown. Police said the suspect left the salon, located in a small strip mall near a Family Dollar store, and then shot himself several miles away at a home on Paradise Lane. Source: http://www.orlandosentinel.com/news/local/breakingnews/os-casselberry-shooting-three-dead-20121018,0,289503,print.story

Communications Sector

Vodafone 'account update' notifications lead to phishing sites. Vodafone phishing emails have been seen landing in inboxes in the past few days, informing customers that they need to update their accounts. Cybercriminals are not only after bank account details. The information stored in accounts that customers register on their mobile carrier's site could be just as valuable. Spammers have started sending out alerts entitled "Your Vodafone accounts update." The link does not point to the legitimate Vodafone site, but a Web page designed to trick users into disclosing their usernames and passwords. By gaining access to their victims' accounts, the scammers also gain access to billing information and other sensitive data that can be used to commit identity theft-related crimes. Source: http://news.softpedia.com/news/Vodafone-Account-Update-Notifications-Lead-to-Phishing-Sites-300149.shtml

Critical Manufacturing

NHTSA recall notice - Ford Fiesta side air bags. Ford announced October 16 the recall of 154,604 model year 2011-2013 Fiesta vehicles, manufactured from November 3, 2009 through September 21, 2012. The vehicles fail to comply with Federal Motor Vehicle Safety Standard (FMVSS) No. 208, "Occupant Crash Protection." The passenger side curtain air bag will not deploy in the event of a side impact collision when the front passenger seat is empty. Although the side curtain air bag system was designed to suppress the side curtain air bag under this scenario, that information is not explained in the owner's guide for these vehicles as required by FMVSS No.208. An occupant in the right rear seating position will not have coverage from the side curtain air bag in a side impact collision when the front passenger seat is empty, increasing the risk of injury to the right rear occupant. Ford will notify owners, and dealers will reprogram the vehicle's software free of charge so that it no longer suppresses the passenger side curtain air bag when the front passenger seat is empty. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V488000&summary=true&prod_id=942768&PrintVersion=YES

Defense/ Industry Base Sector

Nothing Significant to Report

Emergency Services

Prison crowding undermines safety, report says. A recent Government Accountability Office (GAO) report on the Bureau of Prisons says inmate overcrowding undermines the safety of the agency's staff, as well as that of the inmates, the Washington Post reported October 15. The prison facilities are crowded because the inmate population is growing faster than the bureau's capacity. As the prison population grew 9.5 percent from 2006 through 2011, the agency's capacity, increasing at 7 percent, did not keep up. Even with new facilities, the prison population grew from 136 percent of capacity to 139 percent, according to the GAO. While crowding has increased, the inmate-to-staff ratio has gone down. In fiscal year 2010, there were almost 1,700 assaults on bureau staff, according to an April 2011 GAO report. Source: http://www.washingtonpost.com/local/prison-crowding-undermines-safety-report-says/2012/10/15/ab77de02-16fc-11e2-a55c-39408fbe6a4b_story.html

Energy

Solar panel control systems vulnerable to hacks, feds warn. DHS is warning of critical vulnerabilities in a computerized control system that attackers could exploit to sabotage or steal sensitive data from operators of the solar arrays that generate electricity in homes and businesses, Ars Technica reported October 15. A slew of vulnerabilities in a variety of products, including the Sinapsi eSolar Light Photovoltaic System Monitor and the Schneider Electric Ezylog Photovoltaic Management Server, allow unauthorized people to remotely log into the systems and execute commands, warned the Industrial Controls Systems Cyber Emergency Response Team in a recent alert. Other vulnerable devices include the Gavazzi Eos-Box and the Astrid Green Power Guardian. Proof-of-concept code available online makes it easy to exploit some of the bugs. The advisory is based on a report published in September that disclosed SQL injection vulnerabilities, passwords stored in plain text, hard-coded passwords, and other defects that left the devices open to tampering. According to researchers, the vulnerable management server is incorporated into a photovoltaic products from several manufacturers. "All the firmware versions we analyzed have been found to be affected by these issues," the researchers wrote. "The software running on the affected devices is vulnerable to multiple security issues that allow unauthenticated remote attackers to gain administrative access and execute arbitrary commands," the researchers said. Source: http://arstechnica.com/security/2012/10/solar-panel-control-systems-vulnerable-to-hacks/

Food and Agriculture

Dole Fresh Vegetables announced precautionary recall of limited number of salads. October 17, Dole Fresh Vegetables of Monterey, California, voluntarily recalled a limited number of cases of Dole American Blend salad in 12-ounce bags, coded A275208A or B, with a use by date of October 17, and UPC 7143000933. The product may be contaminated with Listeria monocytogenes. The salads were distributed in Illinois, Indiana, Maine, Missouri, New Jersey, New York, Ohio, Pennsylvania, Tennessee, and Wisconsin. The recall is due to a sample of Dole American Blend salad which yielded a positive result for Listeria in a random sample test. Source: http://www.fda.gov/Safety/Recalls/ucm324315.htm

More foods containing Sunland peanut products recalled. Sunland Inc.'s massive peanut butter recall extended even further after the company added whole peanuts to its recall list the weekend of October 13. The extension included products made with both whole peanuts and peanut butter from Sunland. AdvancePierre Foods of Cincinnati recalled various frozen products including Peanut Butter and Jelly Sandwiches, Peanut Butter and Jelly Graham Cracker Sandwiches, and Peanut Butter Cup products produced at its Easley, South Carolina factory between July 17, 2011, and May 18, 2012. Justin's of Boulder, Colorado, expanded its recalled items to include the Natural Honey Peanut Butter Squeeze Packs. The product was sold nationally at supermarkets, the Internet, and in the Starbucks' Protein Bistro Box from March 23, 2010, through September 26, 2012. PureFit of Irvine, California, recalled its Peanut Butter Crunch nutrition bars manufactured between March 1 and July 12, 2012, and distributed nationally through health food stores, grocery stores, and online retailers between March and August, 2012. Creative Energy Foods, Inc. of Oakland, California, recalled its Ridge Bar and Crunch thinkThin brand nutrition bars. The Ridge Bars were sold only on the Internet, and The Crunch thinkThin bars were distributed to retail chains nationwide between March 2010 and October 12, 2012. JagRma LLC of San Diego recalled its NuttZo seven nut and seed butter with best by dates between October 7, 2012, and December 31, 2012. The product was sold nationwide at grocery stores via mail order. Lin-Mar Partners, Inc. of Austin, Texas, recalled its Roasted Peanut with Chocolate Energy Bars and Peanut Butter Trail Mix Protein Bars. The bars were distributed in Texas through Randall's, Tom Thumb, HEB, University of Texas Coop, and Academy retail stores. The Roasted Peanut Energy Bar bears a best by date of November 10, 2012. The Peanut Butter Trail Mix Protein Bar has a best by date of November 11, 2012. Source: http://www.foodsafetynews.com/2012/10/more-foods-containing-sunland-peanut-products-recalled/

Government Sector (including Schools and Universities)

Windows Help files used in attacks against industry and government sectors. To make sure their potential victims do not suspect they are the targets of an attack, cybercriminals often rely on harmless-looking Windows Help files (.hlp) to spread pieces of malware. Symantec reports that in the past period, cyberattacks using this attack vector have been aimed at government and industry sectors. According to researchers, everything starts with a simple email which informs the recipient of a "White Paper on corporate strategic planning." In reality, the attachment is not a white paper, but a cleverly designed Windows Help file. The Help file's functionality permits a call to the Windows API, which allows the attacker to execute code and install other malicious elements. Experts emphasize the fact that this functionality exists by design, it is not an exploit. In the attacks identified so far, cybercriminals were trying to spread Trojan.Ecltys and Backdoor.Barkiofork — pieces of malware often utilized in targeted attacks against government agencies and the industry sector. Most of the threats have been identified in the United States, China, India, and France. Source: http://news.softpedia.com/news/Windows-Help-Files-Used-in-Attacks-Against-Industry-and-Government-Sectors-299782.shtml

(Georgia) **University of Georgia hacked, at least 8,500 employees exposed.** Hackers managed to gain access to the records of at least 8,500 current and former University of Georgia employees, Softpedia reported October 16. The cybercriminals obtained access to the accounts of two employees who worked in "sensitive information technology positions." From there, the attackers were able to gain access to the details of thousands of employees, including names, Social Security numbers, and other information, University of Georgia Today reported. The university's representatives began investigating the breach October 1, after they learned the passwords of two employees were reset by an unknown actor. It was later determined that the intrusion could have occurred as early as September 28. It is believed the hackers might have been able to reset the passwords by guessing the answers to the secret questions set by the targets. All the affected individuals were notified and those who request it will benefit from credit monitoring services. The police were contacted to investigate the incident. Source: http://news.softpedia.com/news/University-of-Georgia-Hacked-At-Least-8-500-Employees-Exposed-299800.shtml

Information Technology and Telecommunications

Blackhole/Zeus threat comes via 'You have blocked your Facebook account' spam. Malicious emails entitled "Verify your account" were spotted by security experts. The alerts are part of a cybercriminal campaign whose main goal is to lure users to Blackhole-infested, Zeus-serving Web sites. Fake Facebook notifications are becoming more and more interesting. Recently, instead of informing potential victims that their accounts were suspended by Facebook, spammers tell users they somehow blocked their own accounts. "You have blocked your Facebook account. You can reactivate your account whenever you wish by logging into Facebook with your former login email address and password" the shady emails read. GFI Labs experts indicate that the links from these messages are designed to take Internet users to compromised Web sites that further redirect them to fake Adobe Flash Player update sites. Source: http://news.softpedia.com/news/BlackHole-Zeus-Threat-Comes-Via-You-Have-Blocked-Your-Facebook-Account-Spam-299745.shtml

High bandwidth DDoS attacks are now common, researcher says. Distributed denial-of-service (DDoS) attacks with an average bandwidth over 20Gbps have become commonplace in 2012, according to researchers from DDoS mitigation vendor Prolexic. In 2011, such high-bandwidth attacks were isolated incidents, Prolexic's president said October 16. Very few companies or organizations have the network infrastructure to handle such attacks. Prolexic released its global DDoS attack report for the third quarter October 17. According to the report, there is an 88 percent increase of attacks from the same quarter of 2011. However, compared to the second quarter of 2012, the number of attacks actually declined by 14 percent. The average attack bandwidth during the third quarter of 2012 was 4.9Gbps, which represents a 230 percent increase compared to 2011, and an 11 percent increase compared to the previous quarter. The average attack during the third quarter of 2012 lasted 19 hours, slightly longer than in the second quarter. The majority of attacks — over 81 percent — targeted the infrastructure layer, while 18.6 percent of attacks targeted the application layer. The top three countries where DDoS attacks originated were China with 35 percent of attacks, the United States with 28 percent, and India with 8 percent. Source: http://www.computerworld.com/s/article/9232487/High_bandwidth_DDoS_attacks_are_now_common_researcher_says

Next-generation malware: Changing the game in security's operations center. Sophisticated, automated malware attacks are spurring enterprises to shift their security technology and staffing strategies. In many new cases, augmentations to malware involves no human author, rather, it is being created by an automated program that continually tweaks known attacks in new ways, so that it will not be recognized by antivirus or intrusion prevention systems. Antivirus (AV) systems work by identifying malware through a blacklist — a database of known viruses, trojans, and other malicious code — and blocking and eradicating any code on the list. The premise of AV technology is that it is possible to identify the unique characteristics of any known malware — its "signature" — and use that signature to prevent it from penetrating the enterprise. However, with new "zero-day" malware being created constantly, AV systems often cannot keep up, and their blacklists have become bloated and slow to perform. This growing problem has spurred many vendors and many enterprises — to begin looking for ways to recognize malware not by how it looks — its known signature — but by how it behaves. Source: http://www.darkreading.com/security-monitoring/167901086/security/security-management/240009058/next-generation-malware-changing-the-game-in-security-s-operations-center.html

Fake ADP benefit services emails lead to malware-serving Websites. Malicious ADP spam runs have been around for a while. Besides the classic "ADP Dealers Services Invoice," "ADP Digital Certificate Expiration," and "ADP Funding Notification," a new type of email was seen hitting the inboxes of unsuspecting Internet users. These emails were analyzed by experts from two different security firms: MX Lab and GFI Software. It was determined that the URL's contained in the bogus messages lead to a fake Adobe Web site that serves malicious elements by leveraging the Blackhole exploit kit. Source: http://news.softpedia.com/news/Fake-ADP-Benefit-Services-Emails-Lead-to-Malware-Serving-Websites-298973.shtml

New malware attacks Android smartphones. October 12, the FBI issued an alert through the Internet Crime Complain Center (IC3) to smartphone users about malware that attacks phones running on the Android operating system. This latest threat to Android phone users, according to the FBI, is a “work-at-home opportunity that promises a profitable payday just for sending out email.” The FBI added that the latest versions of the malware affecting smartphone security are Finfisher and Loozfon. The notification said, “A link within these advertisements leads to a website that is designed to push Loozfon on the user’s device. The malicious application steals contact details from the user’s address book and the infected device’s phone number.” Source: http://www.examiner.com/article/new-malware-attacks-android-smartphones

National Monuments and Icons

(Nebraska) **More sections of State’s national forests reopening.** A large swath of Nebraska’s National Forests and Grasslands are reopening, the Associated Press reported October 15. The U.S. Forest Service said it was rescinding its closure order for most of the 25,000 acres that were shuttered due to massive, late-summer wildfires. A forest supervisor said the closure would remain in effect for a much smaller area where the risk of falling trees and erosion remained high. Source: http://www.kearneyhub.com/news/local/more-sections-of-state-s-national-forests-reopening/article_7f4a7cc2-16c5-11e2-9d60-001a4bcf887a.html

Postal and Shipping

Nothing Significant to Report

Public Health

Hospitals’ computer hardware also suffers from infection. MIT’s Technology Review reported October 17 that hospitals’ computerized equipment—such as patient monitoring systems, MRI scanners, and nuclear medicine systems—are dangerously vulnerable to malware, and many systems are in fact heavily infected with viruses. Due to many of these systems running on older versions of Windows, such as Windows 2000, medical equipment manufacturers often will not support security patches or operating system upgrades for their systems, largely out of concern about whether such changes would require them to resubmit their systems to the Food and Drug Administration for certification. The scope of the problem was the topic of a panel discussion at a National Institute of Standards and Technology Information Security and Privacy Advisory Board October 11. The chief information security officer at Boston’s Beth Israel Deaconess Medical Center told attendees that malware had infected fetal monitors in his hospital’s high-risk pregnancy ward to the point where they were so slow they could not properly record data. The systems have since been replaced with new ones based on Microsoft’s Windows XP. Source: http://arstechnica.com/security/2012/10/hospitals-computer-hardware-also-suffers-from-infection/

FDA tackling medical device security. The U.S. Food and Drug Administration (FDA) is looking for ways to improve how it tracks medical device safety and security issues, such as malware risks, GovInfoSecurity reported October 18. The FDA has taken into account the findings of a recent Government Accountability Office report that recommended the FDA develop a plan to improve post-market surveillance of information security issues in medical devices. “We are reviewing all our processes and procedures and will come out with a plan," said the deputy director of the FDA's division of electrical and software engineering. For example, the FDA is considering whether to toughen requirements related to reporting safety and security issues. The FDA is also reaching out to other federal agencies, including the Department of Homeland Security, to coordinate the tracking of security issues. Source: http://www.govinfosecurity.com/fda-tackling-medical-device-security-a-5210

Meningitis cases climb to 205, deaths to 15. The number of documented U.S. cases of fungal meningitis rose with the Centers for Disease Control and Prevention reporting 205 infections October 14. The latest tally is seven more than the agency reported October 13. The death toll includes the newest fatality, in Indiana; 15 people have died in the outbreak. Meningitis had been reported in 13 States thus far, with Tennessee the hardest hit with 53 documented infections and 6 deaths. One of the cases is a "peripheral joint infection" that specifically affects a joint such as a knee, hip, shoulder, or elbow. Members of Congress expanded an investigation into the outbreak. In a letter to the director of the Massachusetts Board of Registration in Pharmacy, leaders of the House Committee on Energy and Commerce noted the Food and Drug Administration sent the New England Compounding Center a warning letter in 2006 "detailing significant violations witnessed" by investigators the previous year. Source: http://www.cnn.com/2012/10/15/health/meningitis-outbreak-duplicate-2/index.html

Transportation

Nothing Significant to Report

Water and Dams

Corps study cites vulnerabilities in wake of Missouri River flooding. A study released by the U.S. Army Corps of Engineers October 15, said the agency did what it could to manage the historic 2011 flooding on the Missouri River but that more repairs, research, and monitoring are needed to mitigate damage in future high flow years. The flooding began after the Corps released massive amounts of water from upstream reservoirs that had been filled with melting snow and heavy rains. The onslaught lasted for more than 100 days, busting levees, carving gouges up to 50 feet deep, and dumping debris on farmers' fields. The Corps said about $400 million would be spent to fix damage along the Missouri River caused by the 2011 flooding. Most levee fixes are expected to be done before spring of 2013, with work on the dams expected to take longer. More funding might be required for the repairs, but the Corps said it was still evaluating the amount. The study also said more water gauges are needed on the Missouri River. It notes that between 1990 and 2010, 387 gauges that once were monitored by the U.S. Geological Survey were discontinued. Seventeen other gauges now provide less information. Source: http://www.columbiatribune.com/news/2012/oct/16/corps-study-cites-vulnerabilities-in-wake-of/

Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168